

UNITED STATES DISTRICT COURT

for the  
Western District of New York

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)  
Hewlett Packard Laptop Computer, Serial No. 5CD5112BJT  
and  
Apple iPhone, IMEI Number 355792070510725

Case No. 17-MJ-1058

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Western District of New York (identify the person or describe property to be searched and give its location):

Hewlett Packard Laptop Computer, Serial No. 5CD5112BJT and Apple iPhone, IMEI Number 355792070510725, which are more fully described in Attachment A, which is attached hereto and incorporated herein by reference.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): Evidence pertaining to access device fraud, as more fully set forth in Attachment B, which is attached hereto and incorporated by reference herein, concerning violations of 18 U.S.C. §§ 1029(a)(1), 1029(a)(4), 1028(a)(3) and 1028(a)(5).

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 1029(a)(1) & (a)(4) and 1028(a)(3) & (a)(5), and the application is based on these facts: See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of      days (give exact ending date if more than 30 days:     ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

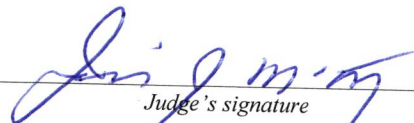
John F. Esau, Jr., Special Agent, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: 6/15/17

City and state: Buffalo, New York



Judge's signature

JEREMIAH J. MCCARTHY, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

STATE OF NEW YORK    )  
COUNTY OF ERIE        )    SS:  
CITY OF BUFFALO        )

I, John F. Esau, Jr., of Homeland Security Investigations, being first duly sworn,  
hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property — two electronic devices listed below — which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am employed as a Special Agent with Homeland Security Investigations (“HSI”), United States Immigration and Customs Enforcement (“ICE”), within the Department of Homeland Security (“DHS”). I have been so employed since July of 2005. I have received training from the Federal Law Enforcement Training Center in Glynco, Georgia. My duties as a Special Agent include the investigation of money laundering, bulk cash smuggling, credit card fraud and wire fraud violations.

3. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

4. The statements in this affidavit are based in part on my investigation of this matter and on information provided by other law enforcement agents and others, as well as my personal observations and knowledge. Where statements of others are related herein, they are related in substance and in part. Because this affidavit is being submitted for the limited purpose of obtaining a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §1029(a)(1), 18 U.S.C. §1029(a)(4), 18 U.S.C. §1028(a)(3) and 18 U.S.C. §1028(a)(5) is located on the electronic devices that the subject of this application and identified below at paragraph 5.

**IDENTIFICATION OF DEVICES TO BE EXAMINED**

5. The property to be searched, identified in Attachment A, includes the following items (hereinafter collectively identified as the "Target Devices"):

- 1) HEWLETT PACKARD LAPTOP COMPUTER, WITH SERIAL NUMBER: 5CD5112BJT ("Target Device 1");
- 2) APPLE iPHONE 6, with IMEI NUMBER: 355792070510725 ("Target Device 2")

The Target Devices are currently in the lawful possession of HSI, having been seized incident to the detention and arrest of Froilan Tressord Bonilla, which is described below at paragraphs 17 to 22. Therefore, while HSI might already have all necessary authority to examine the Target Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws. The Target Devices are currently stored at the HSI facility located at 250 Delaware Avenue, Buffalo, NY 14202. In my training and experience, I know that the Target

Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of HSI.

6. The warrant applied-for would authorize the forensic examination of the Target Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

**BACKGROUND ON ACCESS DEVICE FRAUD AS IT RELATES  
TO "CARDING" AND RE-ENCODED CARDS**

7. Through my training and experience, I know that a common access device fraud scheme known as "Carding" involves the trade and use of illegally obtained personal identification information (PII) and stolen account numbers through online websites, instant messenger services and through "skimming" devices. When fraudulently obtained, these account numbers are Unauthorized Access Devices as defined by 18 U.S.C. § 1029(e)(3)(D). "Carders" include hackers and their distributors who serve as vendors, as well as the consumers who purchase the stolen PII and account numbers and use them. These consumers generally use the stolen PII and account numbers to either purchase goods from online merchants or by manufacturing counterfeit access devices to purchase goods via card present transactions (defined below at paragraph 8(a)).

8. The Credit Card industry has established common standards that govern credit card specifications as well as how transactions using credit or debit cards are processed. This is called the "Payment System," which has the following established standards:



- a. All traditional credit, debit, and gift cards (generally referred to as ‘access devices’) are required to have account numbers embossed or printed on the front of them. These account numbers are also magnetically stored in the magnetic stripe on the back of the card. The magnetic stripe on the card contains two commonly used “Tracks” that contain machine readable information. The account holder’s name is usually only listed on Track 1 and the account number is usually listed on both Tracks 1 and 2. Formatting and other discretionary data is also present on both Tracks. According to industry specifications, the embossed or printed account number listed on the front of the card must match the account numbers encoded on the magnetic stripes. As a result, a card with mismatching account numbers constitutes a Counterfeit Access Device as defined by 18 U.S.C. § 1029(e)(2).
- b. The credit card industry terms “Card Present” transactions as those that are conducted face-to-face between a customer and merchant, in which the card is physically present and used to complete the transaction. A merchant processes a Card Present transaction by swiping the magnetic stripe of a customer’s card through a card reader attached to a Point of Sale (“POS”) Terminal. Only Track 2 is needed to process transactions through the electronic Payment System. Some POS Terminals may read Track 1 and print the account name to the receipt. When the card is swiped, most POS systems mask all of the account information except for the last four digits of the account number, which is often printed on the receipt as well. After the payment is approved,

the merchant is then required to have the customer sign an authorization to complete the transaction. Several merchants have established anti-fraud policies, such as requiring customers to present photo identification matching the name listed on the card, and verifying that the last four digits on the receipt match the last four digits printed on the card.

9. A common Carding commodity is known as a "Dump." A dump is an account number that is arranged in the machine-readable format found on Tracks. A Dump may sometimes be transferred with the victim's name still listed in Track 1. Carders will often either remove this name or add their own or an alias, so merchants do not become suspicious if they see it when conducting a transaction. Carders use Dumps to create counterfeit credit or debit cards. This is often accomplished through a process known as re-encoding. Re-encoding occurs when a carder obtains a stored value gift card or credit card with a magnetic stripe and uses a device known as an "encoder," which attaches to a computer via USB or other connection, and erases or overwrites the card's magnetic stripe transferring the Dump from the computer to the card's magnetic stripe.

10. In my experience, Carders will either encode dumps onto their own legitimately issued cards, or onto counterfeit or altered physical cards, or use gift cards. The advantage to utilizing a card bearing the Carder's true name is that the Carder will be able to produce identification if asked by a merchant. However, this card method is risky in the event that the Carder is caught because his or her true name is on the card. Another method used by Carders is to create counterfeit or altered cards using a manual embosser or printer to emboss or print an account number and name onto the card. This method allows Carders to

choose names and account numbers that would match what the merchant may see when processing the card. The disadvantage to using counterfeit or altered cards is that they may appear altered or lack the security features of genuine cards. Finally, Carders may use the re-encoded gift card method, which has the advantage of not having a name printed on the gift card.

11. Many financial institutions have sophisticated fraud detection policies and mechanisms that allow them to rapidly identify compromised accounts and close them. This prevents further transactions from being processed on an account once fraud has been detected. In response to this countermeasure, Carders often use counterfeit access devices to purchase gift cards. In effect, the funds are removed from the victim's account by the merchant selling the gift card and transferred to a gift card account usually operated by a separate financial institution. This added layer prevents victim financial institutions from tracing and reclaiming their funds.

12. In my experience, once Carders purchase account numbers and PII from hackers or their vendors, they often save the information on their computers' hard drives or other electronic media because they may need to edit and organize it prior to use or distribution. They also often save the information because they don't want to risk losing the information if their computer crashes. In my experience in carding investigations, I have seen carders store account numbers on virtually every form of electronic media. In my experience, carders who possess smart phones often use them interchangeably with their computers. Smart phones have a variety of applications to include email and chat services that Carders often use to procure Dumps. Since smart phones are smaller and easier to travel with than



computers, Carders often utilize their smart phones to conduct and facilitate their Carding activity both at home and while traveling.

13. As a result of the prevalence of card fraud, many merchants have become suspicious of certain types of gift card transactions and have on occasion created their own safeguards to prevent fraud. To counter this, I have learned that Carders often attempt to spread their gift card purchases across multiple stores to avoid detection. They also generally limit the number of gift cards they purchase at one store and may also attempt to purchase items other than gift cards to camouflage their actions. Carders have also been known to make multiple back-to-back purchases of gift cards using different re-encoded cards each time. They are also known to travel long distances, going from town to town along expressways, seeking out stores they are familiar with that sell gift cards. Carders also engage in this practice because it is difficult for store chains and law enforcement to recognize patterns in fraudulent activity when it is spread across many stores and jurisdictions. In my experience, Carders often use GPS (global positioning system) units, or GPS functions and applications that are utilized via smartphones, that allow them to search out particular types of stores in their general vicinity and navigate to them. These waypoints may be retained in the GPS unit or smartphone depending on the model. Finally, knowing that most stores have video surveillance, carders may wear hats or other items meant to obscure their features. Through my experience, articles of clothing observed to be worn by the Carder in video surveillance are often present in their residence. Images of them wearing the clothes may also exist in some form in their own electronic media.



14. Through my training and experience, I know that Carders employ several methods to convert access device fraud proceeds to cash. When Carders purchase gift cards with access devices, they are generally not able to exchange those gift cards for cash through any merchant. Therefore, the Carder's only option is to redeem the gift cards at merchant locations where the gift card is accepted in exchange for goods and services. However, Carders have created other options in order to obtain money for the cards without involving merchants. For example, some Carders sell their gift cards in exchange for cash to individuals/customers on the black market. In this situation, the Carder would typically sell the gift card for less than the face value of the card. Another option used by Carders is to collude with a merchant that has agreed to charge the gift card to their card processing merchant account in exchange for a cash percentage of the face value of the card. Evidence of such transactions are often located on laptop computers and smartphones.

#### **TECHNICAL TERMS**

15. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone), such as Target Device 2, is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling

voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos. Target Device 2 includes a digital camera.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards

or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games. Target Device 2 functions as a portable media player.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision. Target Device 2 includes a GPS antenna and functions as a GPS navigation device.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless

communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device. Target Device 2 functions as a personal digital assistant.

- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks. Target Device 2 includes functions associated with a tablet.
- g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be



assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

16. Based on my training, experience, and research, I know that Target Device 2 has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, PDA and tablet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

### INVESTIGATION

17. On April 10, 2017, Canada Border Services Agency (“CBSA”) refused the entry into Canada of Froilan Tressord Bonilla, Mildred Ramirez Morales, and their minor child. Each of the adults was a Cuban citizen and a Lawful Permanent Resident (“LPR”) in the United States. CBSA advised United States Customs and Border Patrol (“CBP”) that the subjects were in possession of numerous access devices, a laptop computer and a device which was later determined to be a Deftun MSR X6 Magnetic Card Reader/Encoder. CBSA, in

turn, escorted Tressord Bonilla, Ramirez Morales, their minor child, and the vehicle they were driving, to the Peace Bridge Port of Entry (POE) in Buffalo, New York.

18. CBP officers inspected Tressord Bonilla's vehicle and found approximately sixty-five access devices (consisting of credit cards, debit cards, and gift cards), the Magnetic Card Reader/Encoder device referenced at paragraph 17, a Verizon Hotspot device and the Target Devices. Among the sixty-five access devices in Tressord Bonilla's possession, twenty-three had been fraudulently re-encoded. The information encoded on these cards' magnetic stripes was inconsistent with the information on the front of the cards, such as the name on the card, the card number, or the merchant or institution whose name appeared on the card. One of the cards was a MasterCard Debit card issued in Tressord-Bonilla's name but with a magnetic stripe encoded with information that did not match the name and number on the front of the card.

19. HSI Special Agents responded to the Rainbow Bridge Port of Entry and interviewed Tressord Bonilla and Ramirez Morales. Tressord Bonilla claimed that a friend of his, known as "Lazaro Acosta," had asked him to deliver the access devices, Target Device 1, and the reader/encoder to a "Mr. Gonzalez" in New York. Tressord Bonilla was unable to provide a phone number, address or any other way to contact Gonzalez. Tressord Bonilla added that he had intended to meet Gonzalez at a museum, but without a specific date and time. When asked which museum, Tressord Bonilla stated that it was the "National Museum." Tressord Bonilla added that he believed the museum was located "on Broadway," but further stated that he "didn't know New York."

20. Although he claimed that Lazaro Acosta asked him to deliver Target Device 1, along with the other items, to “Mr. Gonzalez,” Tressord Bonilla also said that Target Device 1 had originally belonged to him, that he had sold it to Lazaro Acosta, and that Lazaro Acosta had “loaned” it to him for his trip. In other words, Tressord Bonilla claimed both that Lazaro Acosta asked him to deliver Target Device 1 to “Mr. Gonzalez” and also that Lazaro Acosta loaned him Target Device 1 for his trip.

21. When asked about the MasterCard Debit card that was encoded in his name but held a magnetic stripe with contents not matching the name and number on the front of the card, Tressord Bonilla claimed that he had “lost” the card, and that he “couldn’t explain” why the encoded information did not match the information printed on the card. Later, he added that Lazaro Acosta had given him the card, apparently claiming that after he – Tressord Bonilla – lost the card, the card was somehow re-encoded, found by Lazaro Acosta, and returned to Tressord Bonilla. Tressord Bonilla denied that Ramirez Morales knew anything about the access devices.

22. In her interview, Mildred Ramirez Morales stated that she knew “absolutely nothing” about the access devices. Morales also denied knowing anyone named “Lazaro Acosta.” She said that Target Device 1 belonged to Tressord Bonilla. Morales further stated that she believed that Tressord Bonilla had purchased Target Device 1 approximately two days prior. Morales added that Tressord Bonilla had told her about putting software on Target Device 1. Morales stated that the purpose of the trip was to visit the Cuban embassy in Washington, D.C., which they had done the day before. Morales stated that they were headed to Toronto, Canada, to visit her father.

**ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

23. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, items that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

24. There is probable cause to believe that items that were once stored on the Target Devices may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.



- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

25. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Target Devices were used, the purposes of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Target Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from

a word processing file). With respect to Target Device 1, virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is

a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to engage in carding, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

26. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.


27. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

### CONCLUSION

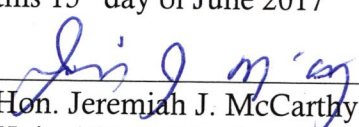
28. Based on all of the foregoing facts, I submit that there is probable cause to believe that a search of the Target Devices will lead to the discovery of the items described in Attachment B (incorporated by reference herein), all of which constitute evidence, fruits, and/or instrumentalities of access device fraud in violation of Title 18, United States Code, Sections 1029(a)(1) [production, use, or trafficking in one or more counterfeit access devices], 1029(a)(4) [production, trafficking, or possession of device-making equipment], and 1028(a)(3) [knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor), authentication features, or false identification documents], and 1028(a)(5) [knowingly



produces, transfers or possesses a document-making implement with the intent such document-making implement be used in production of authentication feature].

  
\_\_\_\_\_  
John F. Esau, Jr.  
Special Agent  
Homeland Security Investigations

Subscribed and sworn before me  
this 15<sup>th</sup> day of June 2017

  
\_\_\_\_\_  
Hon. Jeremiah J. McCarthy  
United States Magistrate Judge

**ATTACHMENT A**

**PROPERTY TO BE SEARCHED**

1. The property to be searched includes the following items (collectively identified as the "Target Devices"):

- 1) HEWLETT PACKARD LAPTOP COMPUTER, WITH SERIAL NUMBER: 5CD5112BJT ("Target Device 1"); and
- 2) APPLE iPHONE 6, with IMEI NUMBER: 355792070510725 ("Target Device 2")

The Target Devices are currently stored at the HSI facility located at 250 Delaware Avenue, Buffalo, NY 14202.

**ATTACHMENT B**

**PARTICULAR ITEMS TO BE SEARCHED FOR AND SEIZED**

1. All records, data and information in whatever format on or within the Target Devices described in the attached affidavit that relate to violations of Access Device Fraud in violation of Title 18, U.S.C. §1029 and other offenses, including 18 U.S.C. §1029(a)(1), 18 U.S.C. §1029(a)(4), 18 U.S.C. §1028(a)(3) and 18 U.S.C. §1028(a)(5):

- a. any and all items, records, documents or communications relating to the sale, purchase or transfer of gift cards, credit cards, debit cards or identification information.
- b. any and all items, records, documents or communications relating to credit cards, debit cards and gift cards, including but not limited to account numbers, names and passwords.
- c. any and all items, records, documents or communications relating to re-encoding of gift cards, credit cards or debit cards, or relating to magnetic card reader/writer device.
- d. any and all items, records, lists, documents or communications relating to personal identification information such as names, addresses, dates of birth, social security numbers, driver's licenses numbers, or any other personally identifiable information that may be used to obtain credit or credit or debit cards or identification documents, including but not limited to address books, names, addresses, phone numbers, email addresses, user names, screen names, mailing lists, supplier lists, and any other contact information.
- e. any and all items, records, documents or communications relating to the advertisement, sale or purchase of merchandise through the use of gift cards, credit cards or debit cards.
- f. any and all receipts and return slips or other records, documents or communications relating to the purchase, sale or return of merchandise or other records relating to transactions made with gift cards, credit cards or debit cards.
- g. any and all computer passwords and other data security device designed to restrict access to or hide computer software, documentation, or data, including

but not limited to programming codes, encryption devices, chips, or programming codes that may create "test" keys or "hot" keys, or which perform certain pre-set security functions when touched;

- h. any and all data and information concerning any Internet and/or cell phone service providers;
  - i. Any photograph, instruction manual, carder instructions, calendar entry, or other item in any format that directly or indirectly relates to the use of unauthorized access device or other supporting activities.
- 2. Evidence of ownership and/or use of the Target Devices identified in Attachment A.
- 3. Any and all communications and records of communications relating to Access Device Fraud in violation of Title 18, U.S.C. §1029 and other related offenses, including 18 U.S.C. §1029(a)(1), 18 U.S.C. §1029(a)(4), 18 U.S.C. §1028(a)(3) and 18 U.S.C. §1028(a)(5), including but not limited to emails, text messages, voicemails and records.
- 4. Records of internet use relating to Access Device Fraud in violation of Title 18, U.S.C. §1029 and other related offenses, including 18 U.S.C. §1029(a)(1), 18 U.S.C. §1029(a)(4), 18 U.S.C. §1028(a)(3) and 18 U.S.C. §1028(a)(5), including but not limited to websites accessed and including but not limited to downloads and browser history.